

CLAIMS

1. In a distributed network of interconnected computing devices, a network virus/worm monitor, comprising:
 - a network virus/worm sensor; and
 - a traffic controller in communication with the network virus/monitor sensor and the network operable in a number of modes wherein in a first mode the bandwidth of the network is substantially unaffected by the traffic controller during a virus/worm sensing operation by the network virus/worm sensor wherein when the network virus/worm sensor detects a computer virus or a computer worm in network traffic, the virus/worm sensor causes the traffic controller to switch to a second mode such that only those data packets infected by the detected computer virus or computer worm are not returned to the network.
2. A monitor as recited in claim 1, wherein those data packets deemed to be infected by the identified computer virus or computer worm are forwarded to a virus/worm analyzer unit coupled to the network computer virus/worm sensor.
3. A monitor as recited in claim 2, wherein in the first mode, substantially all data packets included in the network traffic are copied by the traffic controller.

4. A monitor as recited in claim 3, wherein substantially all of the copied data packets are forwarded to the virus/worm analyzer unit.
5. A monitor as recited in claim 4, at the virus/worm analyzer unit, the copied data packet is forwarded to a packet protocol determinator that determines if the packet protocol of the copied data packet is one likely to be infected by the detected computer virus or computer worm.
6. A monitor as recited in claim 5, further comprising:
 - a trash collector arranged to receive those copied data packets determined to be of a protocol not likely to be infected by the detected computer virus or computer worm;
 - a filescan unit arranged to receive and analyze those copied data packets determined to be of a protocol likely to be infected by the detected computer virus or computer worm.
7. A monitor as recited in claim 5, further comprising:
 - a virus/worm analyzer unit arranged to determine if those copied data packets received at the filescan unit are infected by the detected computer virus or computer worm wherein those packets determined not to be infected are forwarded to the trash collector;
 - a virus analysis unit arranged to analyze the infected copied data packets; and
 - a virus report module arranged to generate a virus report based upon the analysis.

8. A monitor as recited in claim 2, wherein in the second mode, only those original data packets included in the network traffic suspected of being infected by the detected computer virus or computer worm are forwarded by the traffic controller to the virus/worm analyzer unit.

9. A monitor as recited in claim 8, at the virus/worm analyzer unit, the original data packet is forwarded to a packet protocol determinator that determines if the packet protocol of the copied data packet is one likely to be infected by the detected computer virus or computer worm.

10. A monitor as recited in claim 9, further comprising:

a network interface arranged to return to the network traffic only those original data packets determined to be of a protocol not likely to be infected by the detected computer virus or computer worm, wherein the filescan unit receives and analyzes those original data packets determined to be of a protocol likely to be infected by the detected computer virus or computer worm.

11. A monitor as recited in claim 10, wherein the virus/worm analyzer unit determines if those original data packets received at the filescan unit are infected by the detected computer virus or computer worm wherein those packets determined not to be infected are forwarded to the network interface for return to the network traffic and wherein the virus analysis

unit analyzes the infected original data packets and the virus report module generates a virus report based upon the analysis.

12. A monitor as recited in claim 1, wherein the first mode is an inline mode and wherein the second mode is a standby mode.

13. In a distributed network of interconnected computing devices, a method of managing network traffic by a network virus/worm monitor, having a network virus/worm sensor, comprising:

during a virus/worm sensing operation, the bandwidth of the network is substantially unaffected by the traffic controller by the network virus/worm sensor in a first mode wherein when the network virus/worm sensor detects a computer virus or a computer worm in network traffic; and

switching when a computer virus or computer worm is detected to a second mode such that only those data packets infected by the detected computer virus or computer worm are not returned to the network.

14. A method as recited in claim 13, further comprising:
copying substantially all data packets.

15. A method as recited in claim 14, wherein in the first mode, copying by the traffic controller substantially all data packets included in the network traffic; and

forwarding the copied data packets to the virus/worm analyzer unit.

16. A method as recited in claim 15, comprising:
forwarding the copied data packet to a packet protocol determinator; and
determining if the packet protocol of the copied data packet is one likely to be infected by the detected computer virus or computer worm.

17. A method as recited in claim 16, further comprising:
receiving at a trash collector those copied data packets determined to be of a protocol not likely to be infected by the detected computer virus or computer worm; and
receiving and analyzing those copied data packets determined to be of a protocol likely to be infected by the detected computer virus or computer worm at a filescan unit.

18. A method as recited in claim 17, further comprising:
determining by a virus/worm analyzer unit if those copied data packets received at the filescan unit are infected by the detected computer virus or computer worm;
forwarding those packets determined not to be infected to the trash collector;
analyzing the infected copied data packets; and
generating a virus report based upon the analysis.

19. A method as recited in claim 14 comprising:
wherein in the second mode,
forwarding only those original data packets included in the
network traffic suspected of being infected by the detected
computer virus or computer worm are to the virus/worm analyzer
unit.
20. A method as recited in claim 19, at the virus/worm analyzer unit,
forwarding the original data packet to a packet protocol
determinator; and
determining if the packet protocol of the copied data packet is one
likely to be infected by the detected computer virus or computer worm.
21. A method as recited in claim 20, further comprising:
returning to the network traffic only those original data packets
determined to be of a protocol not likely to be infected by the detected
computer virus or computer worm; and
analyzing those original data packets determined to be of a protocol
likely to be infected by the detected computer virus or computer worm.
22. A method as recited in claim 21 comprising:
determining if those original data packets received at the filescan
unit are infected by the detected computer virus or computer worm

forwarding those packets determined not to be infected are to the network interface for return to the network traffic; and
generating a virus report based upon the analysis.

23. A monitor as recited in claim 13, wherein the first mode is an inline mode and wherein the second mode is a standby mode.

24. Computer program product for managing network traffic by a network virus/worm monitor, having a network virus/worm sensor, comprising:

computer code for performing a computer virus/worm sensing operation, the bandwidth of the network is substantially unaffected by the traffic controller by the network virus/worm sensor in a first mode wherein when the network virus/worm sensor detects a computer virus or a computer worm in network traffic;

computer code for switching when a computer virus or computer worm is detected to a second mode such that only those data packets infected by the detected computer virus or computer worm are not returned to the network; and

computer readable medium for storing the computer code.

25. Computer program product as recited in claim 24, further comprising:

computer code for copying by the traffic controller substantially all data packets included in the network traffic.

26. Computer program product as recited in claim 25, wherein in the first mode,
computer code for forwarding the copied data packets to the virus/worm analyzer unit.
27. Computer program product as recited in claim 26, comprising:
computer code for forwarding the copied data packet to a packet protocol determinator; and
computer code for determining if the packet protocol of the copied data packet is one likely to be infected by the detected computer virus or computer worm.
28. Computer program product as recited in claim 27, further comprising:
computer code for receiving at a trash collector those copied data packets determined to be of a protocol not likely to be infected by the detected computer virus or computer worm; and
computer code for receiving and analyzing those copied data packets determined to be of a protocol likely to be infected by the detected computer virus or computer worm at a filesan unit.
29. Computer program product as recited in claim 28, further comprising:

computer code for determining by a virus/worm analyzer unit if those copied data packets received at the filescan unit are infected by the detected computer virus or computer worm;

computer code for forwarding those packets determined not to be infected to the trash collector;

computer code for analyzing the infected copied data packets; and

computer code for generating a virus report based upon the analysis.

30. Computer program product as recited in claim 29 comprising:

wherein in the second mode,

computer code for forwarding only those original data packets included in the network traffic suspected of being infected by the detected computer virus or computer worm are to the virus/worm analyzer unit.

31. Computer program product as recited in claim 30, at the virus/worm analyzer unit,

computer code for forwarding the original data packet to a packet protocol determinator; and

computer code for determining if the packet protocol of the copied data packet is one likely to be infected by the detected computer virus or computer worm.

32. Computer program product as recited in claim 31, further comprising:

computer code for returning to the network traffic only those original data packets determined to be of a protocol not likely to be infected by the detected computer virus or computer worm; and

computer code for analyzing those original data packets determined to be of a protocol likely to be infected by the detected computer virus or computer worm.

33. Computer program product as recited in claim 32 comprising:

computer code for determining if those original data packets received at the filescan unit are infected by the detected computer virus or computer worm forwarding those packets determined not to be infected are to the network interface for return to the network traffic; and

computer code for generating a virus report based upon the analysis.